HEALTH INFORMATION PRIVACY
ALERT

February 2001 • Vol. 5 #2

Editor: Dennis Melamed
Tel: (202) 296-3069
Fax: (202) 466-8032
E-Mail: HIPAlert@aol.com
ISSN# 1099-2066

HHS Hopes for Final Security Rule by June

Quashing rumors that the HIPAA security regulation was being delayed until the end of the year, HHS says it plans to issue the rule by the end of June. Concerns over a delay were generated in part by the Bush Administration's freeze on the regulations and proposals issued in the waning days of the Clinton White House. (HIPA 1/01, p.1)

Such a delay, however, would place extra burdens and expense on healthcare providers, health plans and clearinghouses covered by both the privacy and security provisions unless the privacy rule is delayed as well. (see story, p. 2)

Not Worth the Wait?

Company compliance strategies for privacy necessarily involve decisions on security. Consequently, HHS privacy regulators and covered organizations want to see the security regulation soon.

Some key integration issues for companies include:

✔ **Minimum Necessary** limits on data sharing directly interact with the security proposal's requirements for access controls. Security systems will have to be based on both the amount of information needed by an individual and the security clearance of that individual.

✔ **Audit Trails**. Both the privacy rule and security proposal require audit trails. Under the privacy regulation, audit trails are geared toward sharing information with the patient on who has had access to his or her files. Under the security proposal, audit trails provide an internal mechanism to track who has been accessing protected health information. HHS officials and industry experts are finding that companies are getting the requirements confused.

While the department generally sees these audits as separate concepts, the two are related. Patient requests for a listing of organizations receiving protected health information conceivably could lead to inquiries over who specifically had access to the data. Until specific requirements are outlined for both issues, healthcare companies will find

continued on page 2

Executive Briefing

Free Model HIPAA Privacy, Transaction Standards Contracts Available

Healthcare executives and administrators have free access to a new model business associate contract developed by PrivacySecurityNetwork.com.

Under the HHS privacy regulation, healthcare providers and plans must obtain contractual assurances from those partners and contractors with whom they share protected health information..

The model contract was developed by Alexander J. Brittin, Esq., and sponsored in part by *HIPA*.

The model contract as well as one for the Trading Partner agreement under the HIPAA Transaction Standards regulation, which also mandates contractual agreements, can be accessed at **www.privacysecuritynetwork.com/healthcare** or by calling *HIPA* at (202) 296-3069.

Health Information Privacy Alert is published by Melamedia Editorial Services
8315 Riverside Road • Alexandria, VA 22308

Security

continued from page 1

it difficult to develop integrated systems and policies.

✔ **Paper and Electronic Records.** Only the privacy rule addresses paper records. Until the final security regulation, which is limited to electronic records, is issued, companies will find "an empty spot" with no guidance on how to proceed, one HHS official told *HIPA*.

✔ **Business Associate and Chain of Trust Agreements.** The privacy regulation establishes requirements that covered entities enter into Business Associate contracts committing vendors and partners with whom they share protected health information to abide by the regulation. The proposed security rule has a similar provision requiring a Chain of Trust agreement. A long delay could escalate the costs to companies as the contracts could not be negotiated at the same time.

✔ **Personnel Training.** Both the privacy rule and the security proposal impose training requirements. Because data security and privacy are interrelated, a long delay in the security rule may mean that two rounds of training may be needed rather than one that incorporated both areas.

✔ **Privacy Officers and Security Officers.** The final privacy regulation requires the designation of a privacy officer while the proposed security rule would require an information security officer. One HHS official said that the rules do not require that they be the same person. However, until their responsibilities are detailed in both areas, companies can only make educated guesses on how to divide or share those duties.

Delay Sought in Privacy Rule; Firms Should Continue HIPAA Plans

The privacy regulation may start looking like the internal revenue as the Bush Administration gets tugged in opposite directions by the healthcare industry, consumer groups and two influential members of Congress over whether to reopen the HIPAA rule. However, healthcare organizations should continue planning as the core requirements are not likely to be changed.

Instead, the regulation sets out a general framework for protecting health data. Insiders suggest that such a framework gives healthcare firms some guidance on how to generally proceed. Furthermore, it provides marketing departments with an opportunity to differentiate their respective organizations in the marketplace.

"Privacy has now been incorporated as a measurement of efficiency," HHS said in the rule. With the privacy rule on the table, delays should not stop healthcare firms from incorporating privacy controls in their operations.

Even healthcare organizations who want to reopen the rule endorse the idea of providing better protection for medical information and giving patients new rights.

Unable to Comment

Their comments deal with transition times and some of the mechanics of how to balance the need for privacy with running operations. Concerned over the cost and "aggressive implementation schedule" of the privacy regulation, the American Hospital Assn. (AHA) fired the opening salvo Jan. 31, asking HHS to reopen some parts of the privacy regulation. AHA contended that some provisions in "the new rules were changed unexpectedly and dramatically from the proposed rules and/or in ways that may impede patient care."

On Feb. 1, more than three dozen other healthcare associations sought a delay making the same point. Some of the changes prevented the public or the industry from making meaningful comments and suggestions.

"This fact alone argues for a new public comment period," the healthcare organizations said. Because the proposal was 600 pages long, this argument may carry some weight, and a legitimate argument could be made that "unexpected changes" should not

If the privacy rule is not reopened, HHS's expectations for other HIPAA final rules and proposals are as follows:

First Half of 2001

- ✔ Final Security Rule
- ✔ Final National Employer Identifier
- ✔ Provider and National Health Plan Identifiers

After the First Half of 2001

- ✔ Proposed Electronic Claims Attachments
- ✔ Proposed Enforcement Procedures
- ✔ Proposed Standard for Electronic First Report of Injury (workers compensation)
- ✔ Unique Patient Identifier is on hold

Other Laws that Interact with HIPAA's Privacy Regulation

If the privacy rule is deferred, healthcare still must deal with many other laws regulating disclosure of identifiable health data. In some cases, other laws may be pre-empted by HIPAA or enforcement will be coordinated among relevant agencies. For example, under the Gramm-Leach-Bliley Act, banking regulators and the FTC will work with HHS to harmonize enforcement of the financial privacy provisions and the HIPAA privacy rule. Other laws that come into play include:

- ✔ Americans With Disabilities Act,
- ✔ Children's Online Privacy Act,
- ✔ Clinical Laboratory Improvement Act,
- ✔ Employee Retirement Income Security Act,
- ✔ Environmental Protection Act,
- ✔ E.U. Directive on Data Protection
- ✔ Family and Medical Leave Act,
- ✔ Fair Credit Reporting Act,
- ✔ Federal Substance Abuse Confidentiality Rules,
- ✔ Federal Educational Rights & Privacy Act,
- ✔ Federal Highway Administration rules,
- ✔ Food, Drug & Cosmetic Act,
- ✔ Freedom of Information Act,
- ✔ Gramm-Leach-Bliley Act,
- ✔ National Labor Relations Act,
- ✔ Privacy Act,
- ✔ Public Health Service Act,
- ✔ Rehabilitation Act,
- ✔ Social Security Act (including Medicare & Medicaid), and
- ✔ Workers Compensation laws.

have been unexpected.

At the same time, the General Accounting Office told the Senate Health Committee in a Feb. 8 hearing, that most groups it interviewed "acknowledged that HHS was responsive in addressing many of their comments on the draft regulation."

The groups seeking to reopen the rule, including the Assn. of American Medical Colleges, Blue Cross Blue Shield Assn., Health Insurance Assn. of America, the Federation of American Hospitals and the Pharmaceutical Research & Manufacturers Assn., singled out five problems.

They were "especially concerned" over the effects of a provision requiring patients to sign a specific patient consent before providers could use or disclose protected health information for treatment, payment and healthcare operations. They explained that HHS "went to great lengths" in the proposal to explain why such an approach was unworkable and rejected it.

The rule threatens the patient's ability to get medicine. Pharmacists will be unable to fill or refill prescriptions for consumers, and prescriptions called in by physicians will not be filled unless the pharmacies have written consents on file as the rule stands now, they said.

The groups also wanted HHS to specifically state what it intended by its "minimum necessary" disclosure limits. While pleased the rule excluded disclosures and requests by healthcare providers for treatment, it was "less clear on whether the standard applies to 'use' of information."

This is not "a minor technical detail," the industry groups said. They need "definitive" clarification that the "use" of patient data is not subject to the minimum disclosure rules as well. If this is not provided, they warned that health professionals and trainees in hospitals would be prevented from freely discussing a patient's complete chart to determine treatments.

They also objected to changes to the Common Rule, governing human protection in clinical trials. The administrative costs to gain access to records will "impose significant new burdens" and divert funds from research.

Institutional review boards (IRB) also would be placed in the position of determining when the privacy risks to individuals were reasonable in relationship to the benefits of the research.

"This introduces into the IRB process a determination for which there are no normative standards, and which will of necessity be based on the belief structures and ideologies of individual IRB members," they said.

They cautioned that the transition provisions could "create a potentially chilling scenario" when enforcement of the rule starts in February 2003. They explained that healthcare providers would be unable to use or disclose protected health information for most activities without a signed patient consent. "How providers will obtain consent forms from over 200 million Americans by the compliance date is a staggering problem," they said.

Thomas, Jeffords Want Rule Implemented

Countering these requests, privacy advocates and consumer groups along with House Ways & Means Chairman Bill Thomas (R-Calif.) and Senate Health Committee Chairman James Jeffords (R-Vt.), sent a letter to the Administration asking that the rule not be further delayed. "Americans have already waited too long for federal rules to protect the privacy of their medical records," they said.

AMA Offers 'Measurable' Policies for Privacy, Confidentiality

To help quantify health data privacy protection, the American Medical Assn.'s Institute for Ethics released a consensus report on eight areas in which they have developed "measurable expectations." The report, *The Domain of Health Care Information Privacy*, recommended the use data disclosure boards within organizations as part of a publicly accountable review process.

"Every use of identifiable health information without consent should receive publicly accountable review and oversight," the report said. The authors conceded that while obtaining valid consents for every legitimate use of identifiable health data is not feasible, "every use ...requires some form of accountable review to ensure its legitimacy."

In establishing accountability, the report outlined the following measures for enforcing internal policies:

- ✔ Clear policies and materials for all agents who have access to identifiable health data to support training in the handling of sensitive health information.
- ✔ Individuals handling identifiable health information are properly trained, on a regular basis, in their security and confidentiality standards, including requirements that are specific to each individual's job.
- ✔ Reprimands, feedback, education, probation, and other appropriate methods are used to enforce privacy and confidentiality protection standards.
- ✔ Written policies specify what level of penalty will result from specific breaches of privacy and confidentiality protections.
- ✔ Individuals handling, or with access to, identifiable health information display knowledge of protections afforded this data and the penalties associated with breaching security or confidentiality.
- ✔ Health information trustees have a formal internal mechanism for individuals to report, without fear of reprisal or complaints, inappropriate handling of personally identifiable health data.
- ✔ When an internal review mechanism does not provide a satisfactory resolution, external review of unresolved privacy complaints are available.
- ✔ Health information trustees, unless otherwise prevented by law, require a written statement of adherence to privacy, security, and confidentiality standards from all employees, agents, subcontractors, and outside organizations who wish to gain access to protected health information.

The report can be found at **http://www.ama-assn.org/ama/upload/mm/369/ef_privacy_rpt.pdf**

Suggested Mechanisms Of Oversight for Some Common Uses Of Identifiable Health Information Without Individual Consent

PROPOSED USE OF INFORMATION	OVERSIGHT MECHANISM(S)
Direct diagnostic or therapeutic benefit to patient whose information is at issue	Implied consent based on presenting for care
Payment for diagnostic and therapeutic care for the patient whose information is at issue	Implied consent based on submitting a bill
Research covered by Common Rule	IRB* review (mandatory)
Research not covered by Common Rule	Voluntary IRB review
Quality assurance/quality improvement projects	DDB** review
Public health reporting	Legal standards
Public health research—Common Rule	IRB review
Public health research—not under Common Rule	IRB or DDB review
Marketing	DDB review
Disease management programs	DDB review
Accreditation	DDB review
Fraud detection and deterrence	Legal standards and DDB review
Fraud prosecution	Legal standards and DDB review

*Institutional Review Board
** Data Disclosure Board

Source: AMA Institute for Ethics

HCFA Has Problem Overseeing Contractor Privacy Compliance

HCFA is already suffering from a problem likely to afflict most healthcare organizations who must comply with the business associate provisions of the HIPAA privacy rule: overseeing contractors.

In a January report on the controversial Outcome and Assessment Information Set (OASIS), the General Accounting Office (GAO) said the agency has no system to monitor contractors.

The database, which is generated from information from home healthcare agencies (HHAs), raised howls of protest from privacy and patient advocates because of the intrusiveness of the some of the questions – particularly those dealing with mental health and finances. (*HIPA* 5/99, p. 2)

While it did not eliminate the mental health questions, HCFA did decide to exclude answers to the financial question from data transmitted by the HHAs to the states. At the same time, HCFA maintained the obligation to get this data.

It also continued to require data on patients not receiving Medicaid or Medicare to more effectively compare the costs of care. In a concession to privacy, HCFA has required that identifying patient information, such as name and social security number, be masked.

Generally Consistent with Privacy Act, But...

GAO, the investigative arm of Congress, concluded that the HCFA's privacy policies and procedures were generally consistent with the Privacy Act.

At the same time, "weaknesses in the implementation of these policies" raised concerns. Paramount among those weaknesses was HCFA's failure to routinely monitor contractors and researcher who had access to personally identifiable Medicare information.

HCFA requires state agencies to ensure that access to OASIS data is restricted and data recipients protect patient confidentiality. However, the agency has not inspected the privacy safeguards in place at the state agencies.

According to GAO, HCFA conceded it still had no system in place to monitor whether the parties subject to the data use agreements are complying with their requirements.

"Without an adequate monitoring system in place, HCFA could be hampered in its attempts to prevent the occurrence of problems and provide timely information and corrective action for any that might occur," GAO said.

For example, HCFA did not always clearly inform beneficiaries of the purposes for which the information may be disclosed. HCFA has taken steps to make these disclosures clearer.

HCFA has taken other steps to bolster privacy protections for OASIS data. HHAs and their agents are not allowed to release OASIS data that identifies patients to the public. It also spelled out the following patient rights to:

- ✔ Know why the HHA is asking OASIS questions;
- ✔ Have their personal healthcare information kept confidential;
- ✔ Refuse to answer questions;
- ✔ Look at and request changes to their personal assessments; and
- ✔ Be informed that OASIS information will not be disclosed except as allowed by the Privacy Act.

From a security perspective, the HHAs have been required to submit OASIS data through a private telephone line, which is part of the Medicare Data Communications Network, since October 2000. The network uses a 128-bit encryption standard.

In addition, the network requires several passwords to enter. Users also must know the confidential phone number for the network, the individual user identification number and password for the network, and the HHA-specific user identification code and password for the applicable state system. Passwords must be changed periodically.

The report is found at **www.gao.gov/new.items/d01205.pdf**

Lack of Definition for Genetics Raises Insurer Questions

The fanfare over the mapping of the human genome in February raised a caution by health insurance underwriters who fear that the genetics will fall prey to political demagoguery and result in an expanded definition of genetic information to include information such as the results of routine tests as cholesterol screenings.

The HIPAA privacy regulation is largely silent on the matter, except to strongly acknowledge that the fear of genetic discrimination was a significant motivation for the rule. The regulation, itself, does not treat genetic information differently than other types of data found in a medical record.

The National Assn. of Health Underwriters interpreted

continued on page 6

Genetic Definition

continued from page 5

the privacy regulation as preventing the use of genetic information in the absence of a diagnosis. If a broad definition is crafted, NAHU fears that underwriters would be prevented from conducting what they consider physical tests, including chemical, blood or urine analyses such as cholesterol tests.

If that occurs, consumers ultimately would be forced to pay higher premiums, NAHU warned.

The association has been engaged in a quiet ongoing campaign aimed at HHS and Capitol Hill to clearly define and limit the definition of genetic tests.

"We have seen a disturbing tendency to stretch the definition of genetic information beyond strictly gene testing," said Janet Stokes Trautwein, director of federal policy analysis. "There are many who want to expand the definition to fluids and tissues," she told *HIPA*.

She said Senate proposals in the last Congress contained broad definitions of genetic information. The proponents of such an approach "take great issue with cholesterol screening, claiming that having 'high cholesterol' is not a diagnosis in and of itself and that since it is a metabolite test, it should be included with other genetic tests," NAHU said.

NAHU may already have made some progress for this session. Senate Democrats adopted definitions that appear consistent with NAHU's position in genetic antidiscrimination legislation (S 19) dealing with employers and health insurers in January.

The provisions, part of a larger antidiscrimination package, would amend the Employee Retirement Income Security Act, the Internal Revenue Code, the Social Security Act and the Public Health Service Act to preclude employers and health plans from discriminating against groups on the basis of predictive genetic information.

The bill would prevent health plans, insurers and employers from requesting or requiring individuals to undergo genetic tests and prevents the disclosure of this information to employers, health insurers, third party administrators, the Medical Information Bureau or others that collect, compile, publish this information The bill would not pre-empt state laws with tighter privacy protections.

The bill would define genetic information as information about "genes, gene products, or inherited characteristics that may derive from an individual or a family member of such individual (including information about a request for or the receipt of genetic services by such individual or family member of such individual)."

Genetic tests are defined as analyses of "human DNA, RNA, chromosomes, proteins, and certain metabolites in order to detect genotypes, mutations, or chromosomal changes.

It would not include information about the sex or age of the individual; chemical, blood, or urine analyses of the individual, unless these analyses are genetic tests, or information about physical exams of the individual, and other information relevant to determining the current health status of the individual..

EEOC Gets Railroad to Stop Genetic Testing of Workers

The Equal Employment Opportunity Commission (EEOC) filed its first court action challenging genetic testing Feb. 9 seeking to stop Burlington Northern Santa Fe Railroad to end genetic testing of employees who filed claims for work-related injuries based on carpal tunnel syndrome. The railroad announced Feb. 12 that it would halt the genetic testing immediately.

The incident raised eyebrows within the healthcare industry who saw little value in the testing. However, they did see a major public relations disaster in the making. The case also may provide further impetus in Congress to pass genetic antidiscrimination legislation. (see story above)

The legal action also may give healthcare some insight into what enforcement action may look like for HIPAA privacy violations as the case deals with the receipt and sharing of protected health information.

"As science and technology advance, we must be vigilant and ensure that these new developments are not used in a manner that violate workers' rights," said EEOC Chairwoman Ida Castro.

In a petition, filed in U. S. District Court for the Northern District of Iowa, the EEOC sought to order the railroad to end its nationwide policy of requiring employees who submitted claims of work-related carpal tunnel syndrome to provide blood samples which were then used for a genetic DNA test for Chromosome 17 deletion, which is claimed to predict some forms of carpal tunnel syndrome. EEOC also sought to halt any disciplinary action of the employee who had refused to submit a blood sample.

The commission said that basing employment decisions on genetic testing violated the Americans with Dis-

abilities Act, which requires that medical tests be relevant to specific jobs.

"Any test which purports to predict future disabilities, whether or not it is accurate, is unlikely to be relevant to the employee's present ability to perform his or her job," stated Chester Bailey, the EEOC Milwaukee District Office Director .

Although the railroad said it had halted the practice, the EEOC said it would continue its investigation.

Furthermore, lawsuits lodged by the Brotherhood of Maintenance of the Way Employees on behalf of all affected union members is proceeding for now against the railroad and Athens Diagnostics, one of the companies that performed some of the DNA work.

The case also may raise questions over the protections afforded employees in the Labor Dept.'s ergonomics regulation, assuming that rule is allowed by proceed under the Bush Administration. (*HIPA* 11/00, p.1)

GM, Medscape May Provide HIPAA Laboratory

The healthcare industry may get a good idea of how well the HIPAA regulations on privacy, security and transaction standards will work in practice. General Motors, the largest private purchaser of healthcare services, and Medscape have embarked on a project to get physicians to use Palm OS hand-held devices in program that ultimately aims to provide access to patient records and insurance claims, billing data and other HIPAA-related activities.

In the initial phase, the three-year program will provide hand-held computers to 5,000 physicians for prescribing drugs. They will use Medscape Mobile, which offers physicians downloadable pharmaceutical reference tools and the ability to write prescriptions

GM hopes to reduce medical errors stemming from illegible handwriting by physicians as well as develop more up-to-date methods for ensuring patients do not suffer adverse drug interactions.

The physicians will be drawn from areas with large numbers of GM employees. Providing incentives for physicians, Medscape and GM will provide access to the formularies of other employer plans on the hand-held computer devices to service other patients.

Neither GM nor Medscape has access to medical records without patient or physician authorization, Dr. Arthur Leibowitz, Medscape's Executive Vice President for Digital Health Strategies told *HIPA*. Physicians will use the devices only to write prescriptions and download information to prevent drug interactions and ensure the products are on GM's formulary.

Many of the details are still under development. "This alliance is still very new, and details surrounding the implementation are being worked on each day," a GM spokesman explained.

As experience in the $5-million program grows and wireless technology evolves to allow the devices to interact with desktop computers, the companies expect the program to branch out into other areas covered by HIPAA, such as insurance billing and accessing patient records.

Medscape signed something akin to a Business Associate contract to protect individually identifiable health information as part of its deal with GM, keeping its options open for further expansion of the program.

Leibowitz said GM and Medscape held discussions with the United Auto Workers before proceeding with the project. In 1999, the union inserted medical privacy provisions in its contracts with the major automakers, including GM, expressing concern over dangers posed by electronic records. (*HIPA* 11/99, p. 1)

GM is said to have pre-existing commitments to ensure that it does not have access to these records and will continue to use independent auditors to assess the prescription program.

Violating Privacy May Warrant Stiffer Sentences

Violating medical privacy regulations and laws could reap tougher sentences under a Jan. 26 proposal issued by the U.S. Sentencing Commission.

In trying to consolidate its guidelines on economic crimes, the commission is considering changes that would allow judges to adjust penalties upward when the offense "caused psychological harm, or severe emotional trauma, or resulted in a substantial invasion of a privacy interest."

Leahy Seeks to Close Marketing Loophole

Senator Patrick Leahy (D-VT) said his staff is drafting a bill to close the marketing loophole exposed by privacy advocate Robert Gellman and others. (*HIPA* 1/01, p.2) Leahy's bill would give patients a private right of action where medical data is sold by third parties. The bill also would require patients' consent before marketers could use their records for advertising.

However, the consensus in Washington is that a comprehensive medical privacy law is unlikely to come out of this Congress.

However, changing parts of regulations through legislation is not unknown as Congress halted work on the unique patient identifier by halting funding.

Presidential Panel Calls on Congress To Pass Medical Privacy Law

Congress should pass legislation that assures "sound practices for managing personally identifiable health information of any kind," the President's Information Technology Advisory Committee recommended in a February report *Transforming Health Care Through Information Technology*. However, the HIPAA privacy regulation is not enough. The panel said, ""uncertainties can be dealt with convincingly only by a clear legislative mandate."

That may be the good news for healthcare organizations. The bad news is that the panel concluded that healthcare organizations "are not well prepared to adopt information technology and applications effectively." Not only is the industry decentralized, it lacks the money to make the necessary technological investments.

"We now have sufficient evidence to state that computer-based patient records can substantially improve patient care, outcomes, and costs," the committee concluded. "Yet to date we do not have the national commitment to assure that Americans will reap the benefits of this technology."

The report is found at **www.itrd.gov/pubs/pitac/pitac-hc-9feb01.pdf**

AHA Develops Model Forms for Notice, Consent under HIPAA Privacy Rule

The American Hospital Association developed model consent and notice forms to help hospitals evaluate their current practices regarding protected health information under the HIPAA privacy rule.

To access the model forms, go to **www.aha.org/hipaa/resources/Content/ModelPrivacyNotice.doc**

AHIMA Offers Model Job Description Of Privacy Officer

The American Health Information Management Assn. released a model job description for a chief privacy office for healthcare. Like protected health data, the job calls for the executive to be involved in many aspects of the business, ranging from compliance reviews internally to reviews of business associates.

Privately, some HHS officials suggest that the responsibilities for assuring compliance will take more than one executive. AHIMA did not provide a model salary figure. To access the model, go to **www.ahima.org/hipaa/PrivacyOfficer2001.htm**

Health Information Privacy Alert
Publisher: Dennis Melamed
Editorial Office: 1612 K St., NW • Suite 1210 • Washington, DC 20006
Tel: (202) 296-3069 • **Fax**: (202) 466-8032 • **E-mail**: HIPAlert@aol.com